REMARKS

Reconsideration and allowance of the above-reference application are respectfully requested. Claims 1-35 are pending in the application.

Claims 1, 2, 18, 19, and 28 are amended to correct an informality: the changes are purely cosmetic and do not affect claim scope.

The objection to the drawings is respectfully traversed. The Examiner's attention is directed to page 6, lines 8-9, which states "Reference is made to the attached drawings, wherein ***elements having the same reference numeral designations represent like elements throughout***...." The use of the same reference numeral to identify several items is proper and necessary to identify those elements that are the same. Since the same reference numeral may be used to identify multiple objects, so long as the multiple objects are ***the same part***, the drawings are proper . (See 37 CFR 1.84(p)(4) "The same part of an invention appearing in more than one view of the drawing must always be designated by the same reference character, and the same reference character must never be used to designate different parts.") Hence, the objection to the drawings should be withdrawn.

Claims 1-35 stand rejected under 35 USC §102(e) in view of U.S. Patent Publication No. 2003/0093563 to Young et al. This rejection is respectfully traversed.

As demonstrated below, Young et al. provides none of the claimed features, and discloses no more than what is already described in the admitted prior art. In fact, the Office Action demonstrates a tortured interpretation of Young et al. based on its piecemeal application thereof, as opposed to considering the reference in its entirety as required.

Young describes a multimedia access network device (MAND) 1000 (See, e.g., Fig. 3) that permits delivery of voice, video, and data services over common IP connections while supporting quality of service (QoS) requirements (see, e.g., paragraphs 2, 9, 13). The MAND includes a traffic shaper 100 configured for prioritizing packets for priority queuing and routing (see, e.g., para. 19, 51), and a client access control (CAC) 800 configured for limiting outgoing traffic for WAN traffic and voice traffic to predetermined quantities based on overall available bandwidth (see, e.g., para. 19, 84-88, 138).

The MAND 1000 of Fig. 3 also includes a VPN process 750 in Fig. 3 that enables establishment of a secure VPN tunnel 1810 (Fig. 13) between the MAND 1000 / 1806 and a remote VPN client 1814 (see, e.g., para. 15, 22, 36, 97-98, 123).

However, Young et al. also describes that "VPN authentication and encrypted sessions can be tunneled through the firewall [200 of Fig. 3] for access to an internal network by using a VPN terminator." (Abstract, lines 24-27; see also paragraphs 22, 98, 220). Hence, the encapsulation and encryption of a data packet occurs ***before*** the packets encounter steering by the packet steering resource 700 (see para. 68), or traffic shaping by the traffic shaper 100, and decapsulation and decryption of the encrypted data packet occurs ***only after*** the encrypted packet has passed the packet steering 700 and the traffic shaper 100.

Hence, Young et al. suffers the same problems as described in the Background of the Invention:

> To date the voice and data packets have encountered IPSEC encryption and sequence number assignment prior to being passed to the outbound driver that performs the QoS functionality. Hence, any detection of congestion by the outbound driver causes reordering of packets such that the higher priority packets are at the front of the outbound queue.
>
> Consequently, the decrypting peer, having detected an IPSEC sequence number that is out of order, drops the packets that were received out of order, even though the dropped packet is a valid, secure packet.
>
> (Page 3, lines 17-24).

Young et al. suffers from the above-identified problems because Young et al. neither discloses nor suggests the claimed features in independent claims 1, 10, 18, and 27 of controlling supply of data packets ***to a cryptographic module*** that generates encrypted packets for multiple secure connections. In fact, Young et al. provides only vague references to IPSec encryption for VPN tunneling, without any specific description of how a specific VPN tunnel should be established. Young et al. provides no disclosure whatsoever of the claimed controlling supply of data packets ***to the cryptographic module***, but actually performs QoS congestion control after encryption has been performed.

Hence, Young et al. neither discloses nor suggests the specific features in independent claims 1, 10, 18, and 27 of controlling supply of data packets to a cryptographic module by: (1) assigning, for each of the multiple secure connections, a corresponding queuing module (queuing means in claim 27); (2) reordering, ***within the corresponding queuing module*** (queueing means), the corresponding group of data packets ***associated with the corresponding secure connection*** according to the determined quality of service policy and the corresponding assigned maximum output bandwidth***for the corresponding queuing module***.

Anticipation cannot be established based on a piecemeal application of the reference, where the Examiner picks and chooses isolated features of the reference in an attempt to synthesize the claimed invention. "Anticipation requires the presence in a single prior art reference disclosure of each and every element of the claimed invention, arranged as in the claim." *Lindemann Maschinenfabrik GmbH v. American Hoist & Derrick Co.*, 221 USPQ 481, 485 (Fed. Cir. 1984). Hence, it is not sufficient that a single prior art reference discloses each element that is claimed, but the reference also must disclose that the elements are arranged as in the claims under review. *In re Bond*, 15 USPQ2d 1566, 1567 (Fed. Cir. 1990) (citing *Lindemann Maschinenfabrik GmbH*).

None of these claimed features are disclosed or suggested by Young et al, and therefore the §102 rejection must be withdrawn because the applied reference fails to each and every element as arranged in the claim.

The Examiner's piecemeal application of Young et al. is insufficient to sustain a valid §102 rejection.

Paragraphs 84-87 provide no disclosure or suggestion whatsoever of "***outputting to the cryptographic module*** a corresponding group of the data packets associated with the corresponding secure connection, and according to a corresponding assigned maximum output bandwidth***for the corresponding queuing module***; rather, paragraphs 84-87 describe Client Access Control with respect to Fig. 10, where if a voice caller cannot initiate a call during call setup due to limited capacity ("the bandwidth is not available"), the calling party is sent a "resource unavailable message" such as a "fast busy tone". Hence, Paragraphs 84-87 describe a complete denial of service!

Moreover, Young et a. describes monitoring only total (i.e., aggregate) capacity: there is no disclosure or suggestion of the claimed "assigned maximum output bandwidth for the corresponding queuing module". Paragraph 86 explicitly states that "the number of active calls is compared to the CAC active call counter 1506. If this number is exceeded then a resource unavailable message 1520 is sent 1522 to the requesting device." Further, paragraph 87 states that "the requested bandwidth is compared to the remaining bandwidth available in the CAC bandwidth counter 1510. ... If the bandwidth is not available, a resource unavailable message is sent to the requesting device."

Further, the Examiner's reliance on the "Glossary of Terms" for the definition of a datagram in paragraph 143 fails to provide any disclosure or suggestion of the claimed feature that "each ***encrypted packet*** successively output from the cryptographic module having a corresponding successively-unique sequence number": any assertion that ***a well-known IP datagram*** is a teaching of successively unique sequence numbers assigned by a cryptographic module to successively output encrypted packets is absurd.

For these and other reasons, the §102 rejection should be withdrawn.

In view of the above, it is believed this application is in condition for allowance, and such a Notice is respectfully solicited.

To the extent necessary, Applicant petitions for an extension of time under 37 C.F.R. 1.136. Please charge any shortage in fees due in connection with the filing of this paper, including any missing or insufficient fees under 37 C.F.R. 1.17(a), to Deposit Account No. 50-1130, under Order No. 10-008, and please credit any excess fees to such deposit account.

Respectfully submitted,

Leon R. Turkevich
Registration No. 34,035

Customer No. 23164
(202) 261-1059
Date: January 4, 2006